

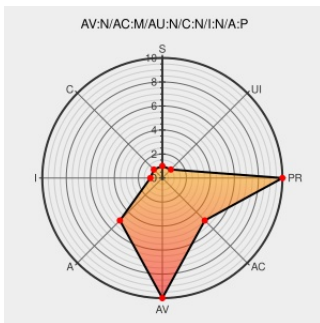


CVE-2008-4323

Published on: 09/29/2008 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:09 PM UTC

CVE-2008-4323

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Windows Xp](#) from [Microsoft](#) contain the following vulnerability:

Windows Explorer in Microsoft Windows XP SP3 allows user-assisted attackers to cause a denial of service (application crash) via a crafted .ZIP file.

CVE-2008-4323 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

**Access
Vector**

NETWORK

**Access
Complexity**

MEDIUM

Authentication

NONE

**Confidentiality
Impact**

NONE

**Integrity
Impact**

NONE

**Availability
Impact**

PARTIAL

CVE References

Description

Tags

Link

Microsoft Windows Explorer - '.zip' Denial of Service - Windows dos Exploit

www.exploit-db.com

[Proof of Concept](#)

[text/html](#)

[EXPLOIT-DB 6616](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows Xp	sp3	unknown	english	All
Operating System	Microsoft	Windows Xp	sp3	unknown	english	All
cpe:2.3:o:microsoft:windows_xp:sp3:unknown:english:*****:						
cpe:2.3:o:microsoft:windows_xp:sp3:unknown:english:*****:						
No vendor comments have been submitted for this CVE						
← Previous ID				Next ID→		